Building Automation Systems—BAS

Terry Martin and Alexandra Bakhto

Introduction

We previously described how the scope of physical security in the information security model extends to include the entire facility as an integrated security system.

The oBIX initiative addressed the convergence of electrical and mechanical systems found in a facility. The automation and connectivity of these systems is collectively called Building Automation Systems, or BAS.

The information security professional must be aware of these systems, because a breach of the network can expose control of the systems to the attacker, and the systems act as information sources that can support the case for security policy.

Building Automation Systems—BAS

BAS leverages information technology to optimize the operation of building systems, including energy management, HVAC, security, fire, elevators, and so on. The controllers associated with BAS are called Direct Digital Controllers (DDC).

Programmable Logic Controller—PLC

A similar technology called Programmable Logic Controllers (PLC) is sometimes found deployed for BAS; however, PLCs differ from DDCs because they tend to be analog and have embedded logic that is configured using ladder logic programming, typically through a non-PC–based interface. PLCs tend to be deployed for rigid high-speed and repetitive applications such as manufacturing automation. PLC programming tends to be short, typically less than 100 lines.

Direct Digital Controller—DDC

DDCs can also have predefined logic; however, because they are architecturally designed to interface with a PC-based application, they tend to be much more flexible, powerful, and user-friendly. A DDC application can be readily identified by the graphical user interface as illustrated here.

DDC controllers operate in stand-alone mode like a PLC; however, because DDC programming is PC-based, extremely complex sequence of operations can be easily constructed.

Most DDC controllers utilize serial communications over industrial networks such as RS-485 and automation protocols such as LonWorks, ModBus, and BACnet; however, IP implementations are common.

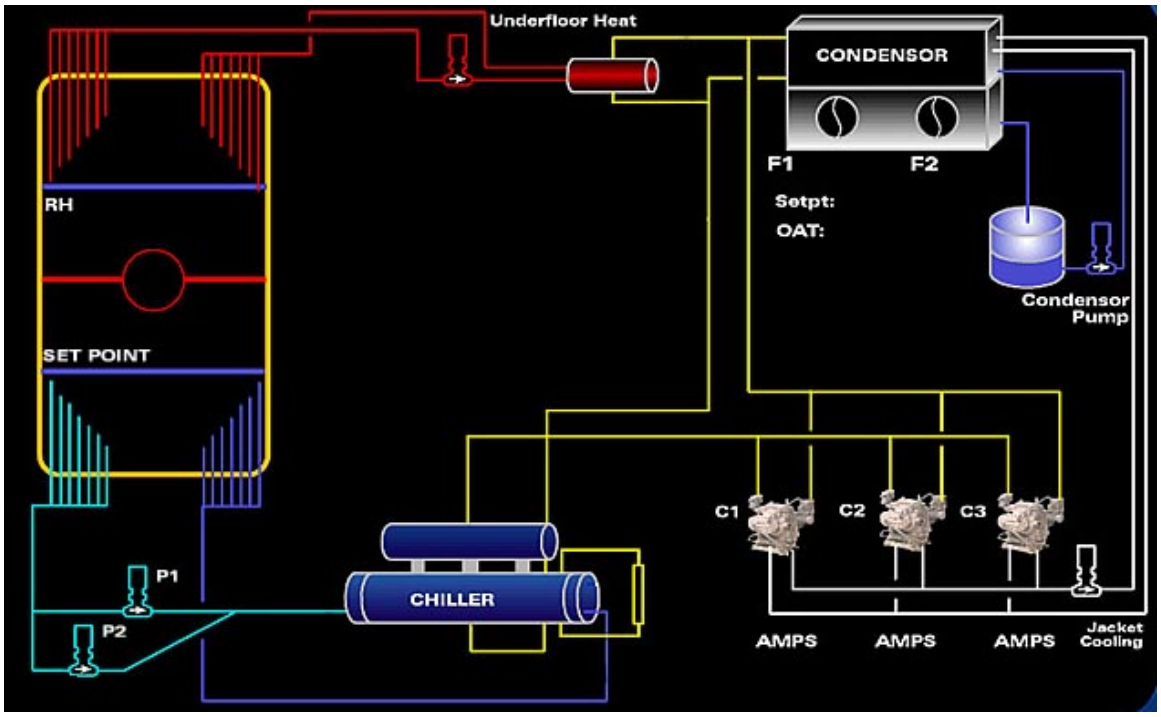

Figure 1: DDC Graphical User Interface

Figure 2: PLC

Figure 3: DDC

The DDC controller is essentially an I/O device with inputs from sensors and equipment, such as temperature and water level, and outputs to various equipment such as HVAC and pumps. Independent systems are logically bridged with the programming, creating an automated sequence of operations to control the building systems.

For example, a fire might trigger the sprinkler system, which might be fed from a roof-top reservoir to maintain pressure. The DDC controller might monitor the reservoir level and switch on auxiliary pumps to top up the reservoir, or shut down ventilation system blowers to prevent smoke from blowing throughout the building.

BAS—CAFM

The BAS systems have an obvious affinity for the graphical environment of the Computer Assisted Facilities Management (CAFM) platform. If the strategy is to advance the CAFM platform as the IT tool set by which the information security budget will be recovered from existing facilities operations, the IT group might find support within a highly technical skill set of the facilities group responsible for BAS.

In addition, BAS systems developers are exposing the data as web services such as XML, making it consumable by both CAFM and Business Intelligence platforms.

Supervisory Control and Data Acquisition—SCADA

BAS has a close relationship to SCADA, although SCADA systems tend to be identified with utilities such as electrical power generation, oil and gas pipelines, water treatment and distribution, chemical processing, and so on.

Threats to SCADA networks are well known, and lessons learned in SCADA network security represent an important model when considering threats in BAS.

Scary examples can be cited, such as the January 2003 incident at Ohio's Davis-Besse nuclear power plant, where the Slammer worm penetrated a private computer network and disabled a safety monitoring system for nearly 5 hours. During the incident, plant personnel continued to be unaware, believing that the network was protected by a firewall.

BAS and SCADA systems have typically placed no priority on security issues, and as convergence progresses, they can constitute a threat that requires serious consideration by the information security professional.

BAS systems have traditionally been supported by dial-up modem connectivity. However, the proliferation of inexpensive broadband Internet connectivity and the tendency for facilities systems to be outside of the scope of the IT group might lead BAS and SCADA systems vendors to simply provision an Internet connection for remote support or monitoring.

It is not unusual to find these systems connected to the Internet with a consumer grade router or directly connected to the ADSL or cable modem. Although a hacked BAS or SCADA system can easily create a life safety risk, the likelihood that the risk is recognized is near zero.

Quantifying the Threat

Although it does not specifically address BAS systems, the British Columbia Institute of Technology maintains a database of SCADA incidents called the Industrial Security Incident Database (ISID).

It is not publicly available; however, it reports there are presently approximately 120 incidents in the database, with an average of 10 added every 3 months.

Summary

The threat presented by BAS and SCADA is well documented; however, as with all information security, new threats emerge with each passing moment. Facilities systems have not traditionally been associated with hacking activity, and awareness is slow to propagate the consciousness of both facilities personnel and support vendors.

By positioning the entire facility as an information security system, the information security professional adopts responsibility for systems not traditionally within the scope of IT skill sets and extends IT security issues into a domain little equipped to deal with it.

Awareness of the threat and close partnering with facilities in a way that results in knowledge transfer is critical to advance the objectives of the information security professional.

Additional Resources

http://terrymartin.info